

## Appendix A - Rules of Behavior

Access to RevCom and any associated applications is granted to you based on certain expectations. These are:

1. Information obtained from RevCom is to be used for official DOE business purposes only.
2. **Authorized Access:** All requests for access must go through the Office of Information Resources, Directives Management Team (MA-90) for authorization.
  - a. MA-90 will then contact the RevCom Helpdesk to coordinate the granting of the appropriate privileges using standard network security constraints and profiles.
  - b. In the event that you no longer require access to RevCom or you leave the employment of DOE or its' authorized contractor organizations, you will notify the RevCom Helpdesk to terminate your user account.
  - c. Any information obtained from RevCom – whether in the form of printed reports or electronic files – is to be protected by you against any purposeful or incidental distribution to anyone not authorized access to such data.
3. **Assignment and Limitations of System Privileges:** The privileges provided to you are adequate to perform the normal functions associated with RevCom.
4. **Dial-In Access:** MA-90 authorizes remote access to some functions in the system only through VPN with a two-factor authentication.
5. **Disposal of IT Resources:** Disposal of IT resources shall be in accordance with current MA-90 or DOE policy and direction. At a minimum, erase fixed media prior to transferring the IT resources or designating the resource for excess.
6. **Individual Accountability:** Never share your logon credentials, userid\password, with anyone.
  - a. Never leave logged on workstations unattended.
  - b. Workstations unattended for 30 minutes or more must be paused.
  - c. Do not logon to more than one workstation/terminal unless you can keep each of them under constant surveillance.
  - d. When access to these IT resources is no longer required, notify MA-90 and make no further attempt to access these resources.
7. **Limits on System Interconnection:** All system changes, regarding the interconnections/interfaces with other system, are under the strict control and approval authority of the CIO and therefore must be coordinated and approved prior to implementation into the production system.

8. **Reporting of IT Security Incidents:** Any unauthorized penetration attempt or unauthorized system use, or virus activity will be reported to your supervisor in accordance with DOE M 205.1-1 (IPWAR Manual).
  - a. Users should also report the security incident to the DOE Headquarters Enterprise Service Center Helpdesk at (301) 903-2500.
9. **Restoration of Service:** Restoration of service is in accordance with the MOU between MA-90 and Doxcelerate Corporation along with the RevCom Disaster Recovery Plan.
10. **Software Installation:** Any request for software installation should be coordinated with your local system/network administration office.
  - a. Only authorized technicians will be allowed to install software on a DOE/COE workstation.
  - b. No personal owned, provided or downloaded software may be installed.
11. **Use of Personally Owned information systems:** Personally owned or provided hardware and/or information systems may not be used to conduct official business.
12. In regards to your **Password** for RevCom access, you agree to follow the following guidelines when changing your Password:
  - a. password contains between 8 and 20 non-blank characters.
  - b. password contains at least one number.
  - c. password must start and end with a letter.
  - d. password must contain at least one special character and can only be either # or \$.
  - e. Password does not contain the user ID.
  - f. Password does not include the user's own or, to the best of his/her knowledge, close friends or relatives names, employee serial number, Social Security number, birth date, phone number, or any information about him/her that the user believes could be readily learned or guessed.
  - g. Password does not, to the best of the user's knowledge, include common words that would be in an English dictionary, or from another language with which the user has familiarity.
  - h. Password does not, to the best of the user's knowledge, employ commonly used proper names, including the name of any fictional character or place.
  - i. Password does not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."
  - j. Password employed by the user on his/her unclassified systems is different than the Passwords employed on his/her classified systems.

Additionally, you agree to protect your Password in the following manner:

- a. Individuals must not share Passwords except in emergency circumstances or when there is an overriding operational necessity
- b. Individuals must not leave clear-text Passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the Password
- c. Individuals must not enable applications to retain Passwords for subsequent reuse.
- d. Passwords must be changed:
  - o at least every 6 months
  - o immediately after sharing
  - o as soon as possible, but within 1 business day after a Password has been compromised, or after one suspects that a Password has been compromised
  - o on direction from management.

### 13. Protection of Personally Identifiable Information (PII)

- o Any remote access to the DOE network to access data in this system must be made through a VPN using two-factor authentication if the data you are accessing is other than your own. Two-factor authentication is where one of the factors is provided by a device separate from the computer gaining access. *Headquarters users need to contact the OCIO to be set up for VPN and two-factor authentication.*
- o All PII media other than your own (i.e., hard copy reports, information loaded to a CD, thumb drive, or any other removable electronic media) that is transported (see definition below) will be encrypted using FIPS 140-2 or greater compliant software. *ICE is the approved encryption software supplied by the OCIO for Headquarters users.*

Transported, in addition to this and/or other electronic transmissions and physical removal, includes sending the information via e-mail and/or accessing the information from your home PC/laptop or DOE laptop or contractor provided PC/laptop from home or any other location not defined as Headquarters (see definition above). Keep in mind that if you view the information from your home or other location, this is considered to be a download and removed from the physical protected Headquarters DOE facility. This would also apply to transporting PII information between DOE protected facilities such as between Germantown and Forrestal.

- o Any and all files that contain PII that are sent via e-mail will be encrypted using Entrust.
- o PII that is stored on Laptops or removable media or at a remote location must be deleted within 90 days or when no longer needed for official DOE business purposes.

**Consequences of Behavior Inconsistent with the Rules:** Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

***I have carefully read and fully understand the explanation of responsibilities and the applicable penalties for failure to abide by the above Rules of Behavior in regards to RevCom.***

---

Signature

---

Print Name

---

Date